

Cryptolocker is back - What you should look for - blueAPACHE

Canonical: <https://www.blueapache.com/blog/cryptolocker-is-back-what-you-should-look-for-2>

Details:

Summary

This blueAPACHE post reports: Another batch of Cryptolocker emails are arriving in inboxes across Australia. Over the past few weeks we have seen five variants – ranging from a poor attempt at a credit card balance email from JP Morgan, to infringement notifications from AFP Australia. It concerns Managed Detection & Response. Published in 2015. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2015
Services referenced	Managed Detection & Response
Topic	Cryptolocker is back - What you should look for

Article

Another batch of Cryptolocker emails are arriving in inboxes across Australia. Over the past few weeks we have seen five variants – ranging from a poor attempt at a credit card balance email from JP Morgan, to infringement notifications from AFP Australia. Those behind the latter seem to think that the Australian Federal Police manage traffic violations. Fortunately, they are easy to identify as fake (hovering your mouse over the links shows the true destination) so they shouldn't cause too many concerns – but they do serve as an opportunity to remind staff that hostage-ware remains prevalent and they need to be vigilant about the links and attachments they click. If you're not familiar with this family of hostage-ware, we have written articles on Cryptolocker , and provided a deep dive into why they will be around for some time to come. The five we have seen are:

1. Refunds from the Australian Tax Office

This attempt does well to mask the sender's email address by making it appear legitimate, but the address seen when hovering your mouse over the link points to a completely different site.

2. Faxes from the Australian Tax Office

This is likely from the same source as the refund statement above. It is only by hovering over the link address that the true destination is seen.

3. Australia Post Delivery notifications

Also replicating the model used in 1 and 2, the sender's email address appears correct, but the link exposed exposed when you hover over the link shows that it is again redirecting you to a another site.

4. Traffic Infringement Notice from the Australian Federal Police

These are a little more obvious. Even if you believe that the AFP are now issuing traffic tickets, the sender's actual email address (traffic-notice24@sdacourier.info) and the link should be enough to alert you something is not quite right.

5. JP Morgan Credit Card Balance

It's unlikely you have a JP Morgan Credit Card, but even if you did – the sender's email address and the link address exposed when hovering the link should be enough to stop you from clicking the link.

More information

For more information on Cryptolocker, click here . For more information on how to better secure your business, speak to the blueAPACHE account team .

Related

Managed Detection & Response
emPOWER Security (pillar)

Frequently asked questions

How many Cryptolocker email variants does the post describe, and what do they impersonate?

The post describes five variants observed at the time: a fake Australian Tax Office refund email, a fake ATO fax notification, a fake Australia Post delivery notification, a fake Australian Federal Police traffic infringement notice, and a fake JP Morgan credit card balance email.

What sender address does the post give as an example of a suspicious link?

For the fake AFP traffic infringement email, the post gives the sender address traffic-notice24@sdacourier.info as an example of an address that should alert recipients something is wrong.

What single check does the post recommend to spot these fake emails?

The post recommends hovering the mouse over links (without clicking) to reveal the true destination address, which it says is enough to expose all five variants as fake.

What does the post say organisations should do about hostage-ware risk generally?

It says these emails serve as a reminder that hostage-ware remains prevalent and staff need to stay vigilant about links and attachments, and points to blueAPACHE's earlier Cryptolocker articles for more detail.

Is this post still current?

No. It describes specific 2015 phishing campaigns. For blueAPACHE's current threat detection services, see the Managed Detection & Response page linked below.

Source

<https://www.blueapache.com/blog/cryptolocker-is-back-what-you-should-look-for-2/>

Knowledge Base

Who wrote the 'Cryptolocker is back' blog post?

The post was written by us.

What are the five Cryptolocker email variants identified in the blueAPACHE article?

The five variants identified are: 1) Refunds from the Australian Tax Office, 2) Faxes from the Australian Tax Office, 3) Australia Post Delivery notifications, 4) Traffic Infringement Notice from the Australian Federal Police, and 5) JP Morgan Credit Card Balance.

How can someone tell that the 'Refunds from the Australian Tax Office' email is fake, ?

The email masks the sender's address to appear legitimate, but hovering the mouse over the link reveals it points to a completely different, illegitimate site.

What clue in the 'Traffic Infringement Notice from the Australian Federal Police' email reveals it as fake?

The sender's actual email address (traffic-notice24@sdacourier.info) and the destination link, visible when hovering over it, indicate the email is not legitimate, especially since the AFP does not issue traffic tickets.